

SUBJECT:

Identity Theft

BROUGHT TO YOU BY:

Nebraska Attorney General

Jon Bruning

WARNING:

fastest growing white-collar crime in the US

Message from Attorney General

Jon Bruning



Dear Friends,

Anyone can become a victim of identity theft. I know because my family has experienced it first-hand! Putting your credit back in order can be a difficult process.

Many victims of identity theft do not even know they are victims until their credit is destroyed. That is why it is important that you understand how to detect identity theft and repair your credit. The goal of this handbook is to arm you with the tools you need to do just that.

The effects of identity theft can be devastating. To minimize the damage done to your good name, you must take immediate action. Use this handbook to guide you through the steps to repair the harm done by identity thieves and prevent identity theft in the future.

Jon

Table of Contents

INTRODUCTION	1
What is Identity Theft?	2
How Do They Get My Personal Information?	3
What Do They Do With It?	3
Identifying Identity Theft	4
 WHEN YOUR IDENTITY IS STOLEN	 7
Immediate Response	
Step 1: File a Police Report	7
Step 2: Close Your Accounts	7
Step 3: Initiate a Fraud Alert	7
Step 4: Fix Specific Problems	11
Step 5: File a Complaint/ID Theft Affidavit	16
 LIABILITY	 19
CHECKLISTS	20
Actions	
Documents	
 PREVENTING ID THEFT IN THE FUTURE	 22
CONTACTS	24

The information contained within this booklet is for educational purposes only and should not be substituted for the advice of an attorney licensed to practice law in Nebraska.



credit denied

WHAT HAPPENED?

You've just come home from a long day at work. The mail is here. More bills. It's just what you need after all the stress from a presentation that is already past deadline. You open your debit card statement. You didn't buy much this month – just some groceries and some clothes. Halfway up the driveway you stop. The statement shows an overdraft. You had more than \$1,000 in your checking account the last time you took out money and now you are more than \$50 in the negative.

You've finally saved up for a car. You've been waiting to get your very own car ever since you graduated from college. You've just picked out a beautiful little blue sports car and the salesman is off putting together the paperwork. Just as you are admiring what will soon be your new ride, the salesman comes up with a sad look on his face. "It's your credit," he says. "I'm sorry."

You finally found the perfect pair of shoes! You can't believe they have your size, too. The salesman rings you up, but there is a problem. Your credit card has been declined even though you hardly use it.

The police knock on your door. They have a search warrant. They inform you that your name, address, and phone number has been connected to a Web site containing child pornography. But you've never built a Web site and you only use your computer for balancing your checkbook and checking your e-mail.

What happened?

You are a victim of identity theft. Someone has obtained access to your checking account or stolen your debit card. Someone has ruined your credit history by opening credit accounts in your name that haven't been paid off. Someone has gotten a hold of your credit card number, either by stealing it, hijacking your computer, or by any number of other ways. Someone has used your personal information to conduct illegal activities. Now that your credit history is ruined and you are in debt for things you never knew about, you can't qualify for an auto loan to buy a car or pay for those perfect shoes. You could be in danger of being arrested for something you didn't do.



WHAT IS IDENTITY THEFT?

Identity theft is when someone fraudulently uses your personal identifying information to obtain credit, take out a loan, open accounts, get identification, or numerous other things that involve pretending to be you.

It is a very serious crime that can cause severe damage to someone's financial well-being if not taken care of promptly. People can spend months as well as thousands of dollars repairing the damage done to their credit history and their name by an identity thief.

Even scarier, some cases of identity theft are connected to other, more serious crimes which may lead law enforcement to you for a crime you did not commit.

How Do They Get My Personal Information?

Identity thieves can obtain your personal information in a number of ways:

- **Finding personal information you share on the Internet;**
- **“Dumpster diving”** or going through your trash looking for personal information;
- **Stealing your mail;**
- **Stealing your wallet or purse;**
- **Stealing your debit or credit card numbers through “skimming”**, using a data storage device to capture the information through an ATM machine or during an actual purchase;
- **“Phishing”**: a scam in which the user sends an email falsely claiming to be from a legitimate organization, government agency, or bank in order to lure the victim into surrendering personal information such as a bank account number, credit card number, or password. This same sort of scam can also be done over the phone by the scammer calling your home;
- **Obtaining your credit report** by posing as an employer or landlord;
- **“Business record theft”** involving the theft of files, hacking into electronic files, or bribing an employee for access to files at a business;
- **Diverting your mail to another location** by filling out a “change of address” form.

What Do They Do With It?

- **Drain your bank account with electronic transfers, counterfeit checks, or your debit card;**
- **Open a bank account in your name and write bad checks with it;**
- **Open a credit card account that never gets paid off**, which gets reflected on your credit report;
- **Use your name if they get arrested** so it goes on your record;
- **Use your name for purchases involved in illegal activities**, such as products for methamphetamine production or an Internet domain for a child pornography site;
- **Use your name to file for bankruptcy or avoid debts;**
- **Obtain a driver’s license with your personal information;**
- **Buy a car and use your information and credit history to get a loan for it;**
- **Obtain services in your name**, such as phone or Internet.

Identifying Identity Theft

Here are some warning signs that you may be the victim of identity theft:

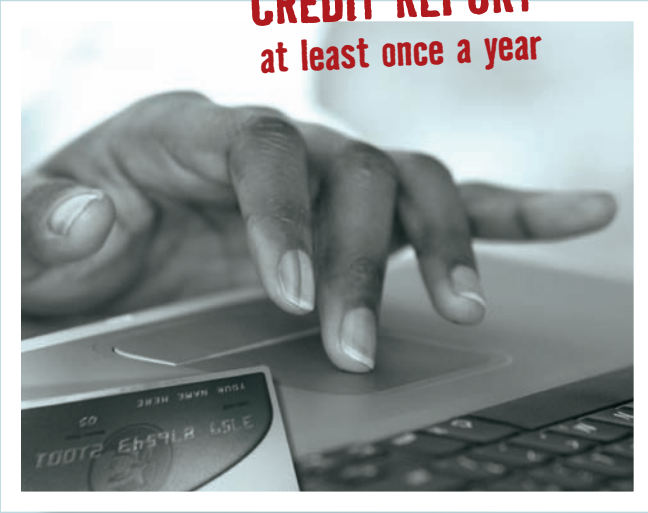
- You are denied credit;
- You find charges on your credit card that you don't remember making;
- Personal information, credit cards, ATM cards, checks, or IDs have been stolen from you;
- You suspect someone has fraudulently changed your mailing address;
- Your credit card bills stop coming;
- You find something wrong with your credit report, such as loans you didn't take out or accounts you don't remember opening;
- A debt collector calls about a debt you don't owe and didn't know about.

If any of these have happened to you, you may be the victim of identity theft.

You could be the victim of identity theft without noticing any of these things happening to you, but it is still good to keep a careful eye out for anything out of the ordinary by ordering your credit report at least once a year and being alert to these warning signs.



**ORDER YOUR
CREDIT REPORT**
at least once a year



A free credit report is available
at www.annualcreditreport.com.



File a police report.

WHEN YOUR IDENTITY IS STOLEN

There are steps you will need to take to protect yourself.

Acting quickly is the best way to make sure that this crime does not get out of control. The longer you wait, the more of your money someone else is spending and, potentially, the greater the damage to your credit.

Always remember to act quickly.

STEP 1: CONTACT THE POLICE

- File a report with your local police department and, if the identity theft did not take place within your area, file a report with the police from the area where the theft took place.
- Get a copy of the police report. You may need that documentation to support your claims to credit bureaus, creditors, debt collectors, or other companies. If you are unable to obtain a copy of the police report, be sure to get the report number.

STEP 2: CLOSE YOUR ACCOUNTS

- If you notice any accounts under your name that have been tampered with or opened without your consent, close them immediately. The longer that an identity thief has access to these accounts, the more money you could lose.
- Call each bank or company and then follow up in writing.
- If there are fraudulent charges or debts on your account or if a new account has been opened, you

should immediately file a fraud report with your bank's fraud department.

- If a new account has been opened without your knowledge and consent, ask the company with which the account has been opened if they have a fraud department. If they do, file a fraud report with that department. If not, ask if they will accept the ID Theft Affidavit from the Federal Trade Commission (see Step 5 page 16).
- If you close an existing bank account and open a new one, be sure to create new PINs (Personal Identification Numbers) and passwords.

STEP 3: INITIATE A FRAUD ALERT

- The next step is to place a fraud alert on your credit file as well as review your credit report. This will prevent an identity thief from opening any more accounts in your name.
- You should contact the three major credit bureaus listed on page 8. If you place a fraud alert with one credit bureau, that credit bureau is required by law to contact the other two bureaus. The other bureaus will include the fraud alert in their reports.
- However, to ensure that the alert is included in your credit file as quickly as possible (to minimize potential damage to your credit history) you should contact all three credit bureaus immediately.

Cont. on next page

INITIAL FRAUD ALERT	EXTENDED FRAUD ALERT
<p>Lasts at least 90 days.</p> <p>It's good if you suspect you might be a victim of identity theft, your wallet/purse is stolen, or if you are a victim of "phishing." With an initial fraud alert, you are entitled to one free credit report from each consumer reporting company.</p>	<p>In your file for 7 years.</p> <p>You can get one on your credit report if you are a victim of identity theft and you have provided the credit bureau with an "Identity Theft Report." This type of fraud alert also entitles you to two free credit reports from each credit bureau within 12 months.</p>

If you lose your Social Security card, contact a credit bureau and have an initial fraud alert placed on your credit reports.

CREDIT BUREAUS
<p>EQUIFAX www.equifax.com</p> <p>P.O. Box 740241 Atlanta, GA 30374-0241 1-800-525-6285</p>
<p>EXPERIAN www.experian.com</p> <p>P.O. Box 9532 Allen, TX 75013 1-888-EXPERIAN (397-3742)</p>
<p>TRANSUNION www.transunion.com</p> <p>Fraud Victim Assistance Division P.O. Box 6790 Fullerton, CA 92834-6790 1-800-680-7289</p>

After you have a fraud alert included in your credit history, you are entitled to receive a free copy of your credit report from each of the credit bureaus. Request a copy and **review your report for the following:**

- Accounts you did not open;
- Debts on your account that you did not know about;
- Inquiries from companies you don't know;
- Inaccurate information.

Contact all three credit bureaus immediately.



Can you believe this is happening?



STEP 4:

Fix Specific Problems

You've identified the problems in your credit report as well as identity theft problems elsewhere. Now it is time to fix them. Here's how:

See *CONTACTS* on page 24 for contact information on these organizations.

EVENT	ACTION REQUIRED	CONTACT
You find any accounts tampered with or opened without your knowledge	Close the accounts immediately. Get new passwords and PINs for new accounts.	Credit Bureaus and creditors (banks, credit card issuers), merchants, utility and cell phone companies
Your ATM card, credit cards, or checks were stolen	Close the accounts immediately. Get new PINs and passwords for new accounts. Notify each bank and major check verification company. If your checks are stolen, put "stop-payments" on all checks remaining in the stolen checkbook. Ask any check verification company to put a fraud alert on your account.	Bank, credit card issuer, creditors, major check verification companies, and the police
You find inquiries on your credit report that you did not know about	By phone and then in writing, notify the three major credit bureaus that unauthorized credit inquiries on your credit history were made and request that those inquiries be removed.	Credit Bureaus
You find inaccurate information on your credit report	By phone and then in writing, notify the three major credit bureaus and request the information be corrected.	Credit Bureaus

Cont. on next page

Step 4: Fix Specific Problems cont.

EVENT	ACTION REQUIRED	CONTACT
You have reason to believe your Social Security Number (SSN) has been stolen or misused	Report your allegations to the Social Security Administration (SSA), request a copy of your Social Security Statement, and/or call SSA to verify the accuracy of the earnings reported on your SSN.	Social Security Administration
An identity thief has falsified change-of-address forms, stolen your mail, or committed any other kind of mail fraud in order to get your personal information	Report it to your local post office. Contact your credit card companies, banks, etc. to notify them that your address was fraudulently changed. Have any changes of address done only in writing.	U.S. Postal Inspection Service (USPIS)
You've lost your passport, it was stolen, or you believe it is being misused	Contact the United States Department of State through a field office or on their Web site.	United States Department of State (USDS)
You think your name or SSN is being used to obtain a fake driver's license	Contact the Department of Motor Vehicles (DMV). Make sure you don't use your SSN as your driver's license number.	Department of Motor Vehicles (DMV)
You think an identity thief has interfered with your security investments or a brokerage account	Report it to your broker or account manager as soon as possible. File a complaint with the U.S. Securities and Exchange Commission.	Your broker/account manager, U.S. Securities and Exchange Commission

EVENT	ACTION REQUIRED	CONTACT
<p>A phone service account has been opened in your name, someone is using your calling card, or unauthorized calls are being billed to your cellular phone</p>	<p>Cancel your account and/or calling card. Use new PINs if you open new accounts.</p>	<p>Your service provider</p>
<p>A debt collector contacts you trying to collect on a loan that you did not take out</p>	<p>Write a letter to the debt collector. State your reasons why you dispute the debt and include supporting documentation, such as a copy of the police report, or the FTC Identity Theft Affidavit.</p>	<p>Debt collector</p>
<p>You have been wrongfully accused of having committed a crime perpetrated by someone pretending to be you</p>	<p>File an impersonation report, have your identity confirmed, and prove your innocence by comparing your information to that of the identity thief.</p>	<p>You may need the assistance of a lawyer, i.e., a criminal defense attorney (public or private) in order to clear your name. Contact the Public Defenders' Office or the State Bar Association in order to find an attorney.</p>
<p>You believe someone has filed for bankruptcy in your name</p>	<p>Write to the U.S. Trustee and include supporting documentation. File a complaint with the U.S. Attorney and/or the FBI.</p>	<p>U.S trustee in the region where the bankruptcy occurred, U.S. Attorney, FBI in the city the bankruptcy was filed.</p>

DON'T WAIT



You can check your credit report online immediately
at www.annualcreditreport.com.

Fixing Your Credit Report

If you find inaccurate information or inquiries on your credit report that you do not know about, contact the credit bureau and request that they be removed.

- First call them and then follow up in writing.
- Provide copies of documents for support. If you cannot get any documentation from the creditor, send the credit bureau copies of your police report.
- Clearly identify what information you are disputing.
- Once your credit report is corrected, ask the credit bureau to send notice of the corrections to anyone who has inquired about your credit report in the last six months.

Creditors

If your credit card was stolen or you find fraudulent charges on your credit card bill, contact the credit card company immediately.

- Close the account as soon as possible.
- Notify the credit card company of fraudulent charges. Have your account number and description of unauthorized charges ready.
- Send the creditor a copy of your police report and a copy of your ID Theft Affidavit (see page 16). If they do not accept the ID Theft Affidavit, fill out the creditor's fraud dispute forms.
- Request a return receipt so that you have proof that the letter was received within the required 60 days after you received the bill with fraudulent charges.

- Remember to keep track of your billing statements. If you do not notify the creditor within 60 days, you may be liable for the fraudulent charges.

See Liability on page 19 for more information.

Social Security Number

If you continue to have problems with an identity thief misusing your Social Security Number (SSN), the Social Security Administration (SSA) can issue you a new number.

- This is not guaranteed to solve your problems.
- A new SSN does not guarantee a new credit record.
- Credit bureaus might combine your new SSN credit record with your old SSN credit record. Even if that does not happen, the absence of any credit history might make it harder for you to get credit.

Also, you cannot get a new SSN if:

- You lost your SSN card or it was stolen, but there is no evidence it is being misused;
- You filed for bankruptcy;
- You are planning on avoiding the law or legal responsibility.

Criminal Violations

If an identity thief has impersonated you when they were arrested or cited for a crime, there are things you can do to correct your record.

- To prevent being wrongfully arrested, carry copies of documents showing that you are a victim of identity theft, whether your name has been used for criminal activity or not.
- If your name has been used, contact the law enforcement agency (police or sheriff's department) that arrested the identity thief. Or if there is a warrant for arrest out for the impersonator, contact the court agency that issued it.
- You may also want to get a lawyer to help you.

STEP 5: Filing A Complaint

The Federal Trade Commission is the federal consumer protection agency.

- The FTC, in conjunction with the FBI, maintains an Identity Theft Data Clearinghouse.
- The FTC aids identity theft investigations by collecting complaints from identity theft victims and sharing the information with law enforcement agencies, credit bureaus, companies where the fraud took place, and other government agencies.
- File a complaint with the FTC by going to www.consumer.gov/idtheft or by calling their toll-free number: 1-877-ID-THEFT (1-877-438-4338).

Identity Theft Affidavit

A piece of documentation you need to fill out is the Identity Theft Affidavit offered by the Federal Trade Commission.

- This form will help you report information about your identity theft with just one form. Many companies accept this form, though others will require you to use their own form.
- If a new account has been opened in your name, you can use this form to provide the information that will help companies investigate the fraud.
- Once you have filled out the ID Theft Affidavit, mail a copy to any of the companies concerned with the fraud you describe in the form, such as banks or creditors.
- The ID Theft Affidavit as well as more detailed information about filling it out can be found at www.consumer.gov/idtheft.

Make sure that you keep copies of all of your paperwork including records of everyone you have corresponded with, fraudulent bills, police reports, and complaint forms.



FILE

**A COMPLAINT
WITH THE FTC**

**the FASTER you act
THE LESS
LIABLE
YOU ARE**



LIABILITY

To ensure that you don't end up paying hundreds or even thousands of dollars in fraudulent charges made by an identity thief, the best course of action is to act quickly. The faster you act, the less liable you are for unauthorized charges.

Credit Cards

According to the Truth in Lending Act, your liability is limited to \$50 in unauthorized credit card charges per card in most cases. In order for this to come into effect, however, you must write to the creditor within 60 days of receiving the first bill that contained the fraudulent charge. If an identity thief changed your mailing address, you must still send your letter within 60 days of when you were supposed to have received your bill.

ATM/Debit Cards

If your ATM or debit card is lost or stolen, report it as quickly as possible. If you report it within two business days, you are only responsible for \$50 in unauthorized withdrawals or transfers.

If you report it between two and 60 days after, you may be responsible for up to \$500 in unauthorized withdrawals or transfers the thief may make. If you do not report it after 60 days, you can lose any money the thief withdraws or transfers from your account.

report within 60 days

CHECKLISTS

Plan of Action List

Because this is a lot of information to take in, we have provided you with a checklist to go through to make sure you have taken all the necessary steps after becoming an identity theft victim. Remember, you must complete all of these steps in a timely manner to minimize your losses.

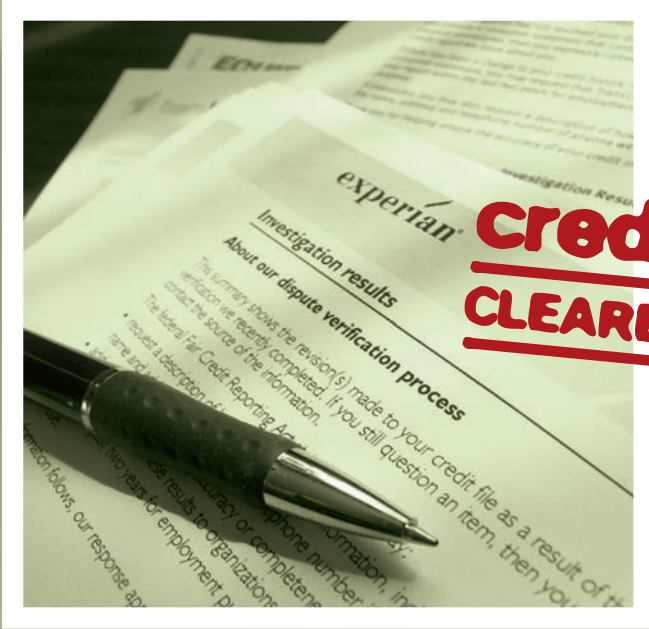
- ☐ 1. Filed a police report.
- ☐ 2. Obtained a copy of your credit report.
- ☐ 3. Identified errors and inquiries you did not know about, accounts you did not open, debts you did not know about, or anything else that seems wrong or out of place on your credit report.
- ☐ 4. Placed a fraud alert on your credit report.
- ☐ 5. Closed any accounts that might have been tampered with or opened without your knowledge or consent.
- ☐ 6. Contacted a major credit bureau by phone and by writing to correct inaccurate information.
- ☐ 7. Filled out the FTC Identity Theft Affidavit.
- ☐ 8. Contacted the correct agencies to fix inaccurate information, close accounts, or report identity theft.
- ☐ 9. Filed a complaint with the Federal Trade Commission.

Document List

Here is a list of documents you should have. You won't be able to keep the originals of some of the documents so it is very important that you make a copy for yourself.

It is also a good idea to keep copies of the documents that prove you are an identity theft victim with you, such as a copy of your police report.

- ☐ 1. Police report
- ☐ 2. Identity Theft Affidavit
- ☐ 3. Bills with fraudulent charges
- ☐ 4. Documentation of accounts opened in your name without your consent
- ☐ 5. Copies of letters sent to credit bureaus and creditors



PREVENTING ID THEFT in the future

No matter how many precautions you take, identity thieves can find a way to steal your identity. But there are precautions you can take to minimize your risk for identity theft and help you catch identity theft quickly.

- 1 Place passwords on bank, credit card, and phone accounts:** Don't use a password that could be easily guessed, such as your pet's name or your birth date and choose a password that mixes random numbers with letters.
- 2 Don't carry your Social Security card:** Don't even carry the number on you. Don't use it as your driver's license number either. Keep the card in a safe place and use the number only when necessary.
- 3 Order a copy of your credit report:** Order a copy from each of the three credit bureaus each year. A credit report contains information on where you live, where you work, how you pay your bills, whether you've ever been sued, arrested, or ever filed for bankruptcy, and what credit accounts have been opened in your name. Reviewing your credit report can alert you to any fraud or errors. This is very important and one of the best ways to catch identity theft. You are entitled to one free credit report annually from each of the three major credit reporting bureaus. Take advantage of it.

234567890

4 Pay close attention to billing cycles: If a bill does not arrive on time, it is possible that an identity thief may have taken it, so remember to check with creditors about a late bill.

5 Guard your mail from theft: Instead of leaving your mail to be picked up in an unlocked mailbox, take it to the post office or leave it in a post office collection box. Make sure you remove your incoming mail right away. Try not to leave mail in your mailbox overnight.

6 Don't give out personal information over the Internet, on the phone, or through the mail unless you have initiated the contact or you are sure about the identity of the person or company. Be aware of schemes such as "phishing" in which the identity thief pretends to be from a legitimate organization or business in order to retrieve personal information from you. This might include calls or emails from someone claiming to be from your bank needing to confirm your Social Security number or bank account number. Be aware of promotional scams that use phony offers as a way to obtain personal information.

7 Keep your information safe online: Only send your personal information, such as your credit card number, over a secure connection (a secure connection has an address that begins with "https" and has a small padlock at the bottom of the page. A window should

also pop up telling you that the Web site is secure). Make sure you have virus protection that you update regularly. Use a firewall program to protect your computer from being accessed by others, especially if you have high-speed Internet which keeps your computer connected 24 hours a day, and a secure browser. You may also want to unplug your Internet while you are not using it. Don't download any files or click on links sent to you by people you don't know.

8 Be wary of "pharming" scams: Pharming happens when you type in the address for a legitimate bank or e-commerce Web site and get rerouted to a copycat Web site. Identity thieves use this scam to obtain your personal information when you log into the Web site. **Here are some ways to spot pharming:**

- Highlight text. The Web site is a copycat if the blocks of text are actually images.
- Look for spelling or grammatical errors.
- Links on the page don't work.
- You should never be asked to verify information.
- Legitimate log-in pages should be encrypted so you should see a padlock at the bottom of the browser and the address should begin with "https". You can click on the padlock to make sure the site's security is registered to the right company.



CONTACTS

Nebraska Attorney General's Office

www.ago.ne.gov

2115 State Capitol
Lincoln, NE 68509

For complaints call:
(402) 471-2682 (Lincoln)
(800) 727-6432 (Toll Free)
Fax: (402) 471-3297

Federal Trade Commission (FTC)

www.consumer.gov/idtheft

FTC
Consumer Response Center
Room H-130
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580
1-877-ID-THEFT (1-877-438-4338)

Major Credit Bureaus

EQUIFAX: www.equifax.com
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-525-6285

EXPERIAN: www.experian.com
949 West Bond Street
Lincoln, NE 68521
1-888-EXPERIAN (397-3742)

TRANSUNION: www.transunion.com
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790
1-800-680-7289

A free copy of your credit report
is available from the website
www.annualcreditreport.com

Or write to:
Annual Credit Report Request Service
P.O. Box 105283
Atlanta, Georgia 30348-5283

Or call: 1-877-322-8228
TDD: 1-877-730-4104

Major Check Verification Companies

To find out if an identity thief has
been passing bad checks in your
name: SCAN: 1-800-262-7771

To request a copy of your consumer
report specifically about your
checking account: Chex Systems, Inc.
at 1-800-428-9623 or
www.chexhelp.com
Attn: Consumer Relations
7805 Hudson Rd., Suite 100
Woodbury, MN 55125

To request that your checks not be
accepted by retailers:

Certegy, Inc. (previously Equifax
Check Systems) at 1-800-437-5120

TeleCheck at 1-800-710-9898 or
1-800-927-0188

Social Security Administration

www.ssa.gov

SSA Fraud Hotline
P.O. Box 17768
Baltimore, MD 21235
SSA Fraud Hotline: 1-800-269-0271

U.S. Postal Inspection Service

[www.usps.gov/websites/depart/
inspect](http://www.usps.gov/websites/depart/inspect)

Call your local post office to find the
nearest USPIIS district office.

Nebraska Department of Motor Vehicles

Visit this Web site to find the DMV
service center closest to you:
**Nebraska DMV Fraud Investigation
Section:** www.dmv.state.ne.us

NEBRASKA ATTORNEY GENERAL'S OFFICE		www.ago.ne.gov
Lincoln	402.471.2682	Toll Free 1.800.727.6432

Nebraska Attorney General's Office
PO Box 98920
Lincoln, NE 68509
11-60-00

PRSRT STD
U.S. POSTAGE
PAID
LINCOLN, NE
PERMIT NO 212



**WE ARE HERE TO
HELP YOU!**

☒ **YES! I WANT TO HELP STOP
IDENTITY THIEVES!**

Fill out the information below and return
the postcard to receive e-mail updates and
other useful information on how you can
protect yourself.

Name

Address

City State Zip

Phone

Email address



Jon Bruning
Attorney General

Consumer
Protection Line

1-800-727-6432
(Toll-free in Nebraska)